Аннотация дисциплины Б1.Б.25
«Теоретико-числовые методы в криптографии»
Общая трудоемкость изучения дисциплины составляет 4 ЗЕТ (144 часа)

Цель изучения дисциплины – дать будущим инженерам, специализирующимся в области защиты информации, основы знаний о принципах защиты информации с помощью теоретико-числовых методов криптографии.

Для достижения цели ставятся **задачи:**

- дать студентам основы системного подхода к организации защиты информации, передаваемой и обрабатываемой техническими средствами, на основе применения криптографических методов;
- дать студентам основы принципов анализа и синтеза шифров;
- ознакомить студентов с математическими методами, используемыми в криптографии;

Основные дидактические единицы (разделы):

Основные целочисленные алгоритмы. Квадратичные вычеты и невычеты, квадратичный закон взаимности Гаусса. Асимптотический закон распределения простых чисел. Методы разложения чисел на множители. Криптографическая система RSA. Протокол Диффи-Хеллмана. Компетенции, приобретаемые в процессе изучения дисциплины.

Компетенции, приобретаемые в процессе изучения дисциплины

способностью корректно применять при решении профессиональных задач аппарат математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории алгоритмов, теории вероятностей, математической статистики, теории информации, теоретико-числовых методов (ОПК-2);

способностью к самостоятельному построению алгоритма, проведению его анализа и реализации в современных программных комплексах (ОПК-10).

способностью участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации (ПК-5);

способностью оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации (ПК-10);

В результате изучения дисциплины студент должен:

Знать:

- основные целочисленные алгоритмы;
- криптографические средства и системы защиты информации и их программно-аппаратную реализацию;
- современные тенденции развития средств и методов криптографической защиты информации;

- основные методы и средства криптографического анализа;

Уметь:

- использовать свойства криптографических средств при анализе комплексных систем защиты информации;
- использовать теоретико-числовые методы криптографии при анализе комплексных систем защиты информации;
- практически решать задачи защиты программ и данных криптографическими средствами;
- оценивать уязвимость протоколов и интерфейсов компьютерных систем;

Владеть:

- алгоритмами дискретного логарифмирования;
- законом распределения простых чисел;
- квадратичным законом взаимности Гаусса;
- методами разложения чисел на множители.

Виды учебной работы:

Семестр	Часов							ЗЕТ
	Всего	Контактная работа (по уч. зан.)				Самост. работа	Контроль	
		Всего	Лек	Лаб	Пр			
9	**72**	36	18		18	36		2
А	**72**	36	18		18	36		2

Изучение дисциплины заканчивается